UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,883	01/20/2004	Richard Paul White	011-CON1	4242

36215 7590 07/03/2008

HAW-MINN LU
10733 CALSTON WAY
SAN DIEGO, CA 92126

EXAMINER	
MEJIA, ANTHONY	
ART UNIT	PAPER NUMBER
2151	
MAIL DATE	DELIVERY MODE
07/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/761,883	WHITE ET AL.	
	Examiner	Art Unit	
	ANTHONY MEJIA	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☒ Claim(s) *1-15* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 February 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/29/2008 and 04/14/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to Application No. 10/761,883 filed nationally on 20 January 2004. The amendment presented on 02 February 2008, which provides change to claims 1-15, is hereby acknowledged. The additional Claims 16-20, are also acknowledged. Claims 1-20 have been examined.

Claim Objections

2. Claims 1-15 are objected to because of the following informalities: content of claim language. In the instant case, for example, claim 1 recites the acronyms: “MTA_0", “MTA_1”, “IP_0”, “IP_1”, “A_0”, "A_1", and “RCPT”. For example, the acronym, “A_1”, claim 8 identically recites the same acronym, but fails to clearly define the acronym. An acronym as such should be defined at least once in each independent claim before use of the acronym in the dependent claims. Same objection applies to the other acronyms used in Claims 14-15. Examiner suggests rewriting and spelling out all the acronyms and/or the definition of all the acronyms and/or commands abovementioned in the at least independent claims. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-13, rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In this case, the amended whereby clause in claim 1 that recites: "whereby the connection with MTA_0 is rejected by the intercepting means before the data portion of the unsolicited message is *transmitted*", raises uncertainties as to whether the connection is rejected before the data portion of the unsolicited message is *transmitted to* the unsolicited message rejecting communications processor or the MTA_1. For the purposes of further examination the examiner will interpret that the connection with MTA_0 is rejected before the data portion of the unsolicited message is transmitted to MTA_1.

Claims 2-13 are also rejected as inheriting the same deficiency through their dependency.

5. Claim 15 is also rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In this instant case, step w) recites: “testing if DD_0 does not match the domain of A_0 and the domain of A_0 is in the suspect_domain database". There is insufficient antecedent basis for this limitation in the claim. For the purposes of further examination, the Examiner will interpret the terms “domain of A_0” as

being synonymous to the terms "sender_address of A_0". Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-5, 7, 9, 11, 14, and 16-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Donaldson (US 7,249,175).

Regarding Claim 1, Donaldson discloses an unsolicited message rejecting communications processor (proxy 1401 of Fig. 13) connected to message transfer agents (remote 1400, local MTA 1402 of Fig. 13),

MTA_0 with an Internet address of IP_0 (IP address of remote host) (col.15, line 50-56), sender_address A_0 ("MAIL From address"), declared domain of D_0 ("MAIL From domain") (col.20, lines 1-5), and real_domain of DD_0 (col.18, lines 11-20, and *see* table 1, and fig.25), and

MTA_1 with an Internet address of IP_1 (destination IP address) (col. 2, lines 61-63, col.9, lines 19-27) and recipient A_1 (To: address) (col.34, lines 51-52) comprising:

a) monitoring means (proxy 1401 on fig. 13) for monitoring the communications between MTA_0 and MTA 1 (wherein the proxy is provided in a conventional firewall configuration i.e., monitors transfers of information, between MTA_0 e.g., a remote host and a MTA_1 e.g., local MTA (col.8, lines 25-28);

b) determining means (proxy 1401 on fig.13) for determining if the communications contains an unsolicited message (proxy determines if the communication contains an unsolicited message by determining if the email contains trusted addresses, where if it does not contain trusted addresses (e.g. trusted hosts or white-listed addresses) it is deemed junk mail, i.e., it contains addresses of the purported sender which is commonly forged in junk mail. (col.15, lines 50-65); and

c) intercepting means (proxy 1401 on fig. 13) for intercepting (e.g. receiving) a RCPT command from MTA_0 (step 1631 of Fig. 26, col. 40, lines 29-45) and sending an error reply (e.g., response 550) to MTA_0 if the message is determined to be unsolicited (step 1655 of fig. 27),

whereby MTA_1 controls the interaction between MTA_0 and MTA_1 (e.g. step 1015 in fig. 2 for accepting/rejecting messages there from), before a RCPT command from MTA_0 is received by the unsolicited message rejecting communications processor (e.g., proxy 1401, may be implemented at the MTA

level, col. 3, lines 51-60, col.8, lines 21-24, col.9, lines 19-27, col.14, lines 5-22, col.17, lines 45-54, and col.36, lines 6-15) and

whereby the connection with MTA_0 is rejected before the data portion of the unsolicited message is transmitted (e.g., closing the connection when proxy suspects that a sender's address was forged and col.16, lines 56 or if the remote host address is blacklisted the proxy closes the connection and exits without any email being transferred, col.19, lines 23-26).

Regarding Claim 2, Donaldson teaches an allow_address database (e.g., trusted database) and wherein the determining means (proxy 1401 on fig. 13) for determines if a message is not unsolicited by checking if the address IP_0 is in the allow_address database (e.g., trusted database 1093 of Fig. 7, is used to identify trusted networks (IPs) that are permitted to bypass further filtering, col.11, lines 58-60).

Regarding Claim 3, Donaldson teaches a prevent_address database (e.g., blacklist database 1095 of Fig. 7) and wherein the determining means (proxy 1401 on fig. 13) determines if a message is unsolicited by checking if IP_0 is in the prevent_address database (e.g., blacklist, identifies IP addresses of remote hosts that will be blocked immediately after they connect to the proxy server, col. 11, lines 62-63).

Regarding Claim 4, Donaldson teaches access to a open relay database (e.g., relay database 1096 of Fig. 7) and wherein the determining means (proxy 1401 on fig. 13) determines if a message is unsolicited by checking if IP_0 is in the open relay database (e.g., relay database including addresses of untrusted hosts that are known not to be dialup clients col. 11, lines 64-67).

Regarding Claim 5, Donaldson teaches access to a DNS (domain name server) database (e.g., configuration database 1098 of Fig. 7) and wherein the determining means (proxy 1401 on fig. 13) determines if a message is unsolicited by checking if IP_0 has a domain name entry DD_0 in the DNS database (e.g., configuration database, which includes general data such as permissible domain names, col.12, lines 1-4, col.16, lines 21-31).

Regarding Claim 7, Donaldson teaches where the unsolicited rejecting communications processor further includes a suspect_domain database (configuration database 1098 of fig.7) and

wherein the determining means (proxy 1401 on fig. 13) determines if a message is unsolicited by checking if the actual domain DD_0 matches the domain of from-address A_0 (col.16, lines 21-31, col.15, lines 60-67, and col.16, lines 1-4) Donaldson further teaches where the proxy is compatible with all known SMTP MTAs. Therefore, an MTA itself (not shown in figures), can also provide additional filtering functionalities such as rejecting non-existent MAIL From domains, col. 9, lines 19-27) and the domain of from-address A_0 is in the

suspect_domain database (configuration database 1098 of fig.7) (col.16, lines 20-31).

Regarding Claim 9, Donaldson teaches a no_filter database (e.g., recipient whitelist 1600) and wherein the determining means (proxy 1401 on fig. 13) if the message is to be blocked if it is determined to be unsolicited by checking if the recipient A_1 is in the no_filter database (e.g., whitelist 1600) (col.37, lines 29-32)

Regarding Claim 11, this method claim comprises limitation(s) substantially the same, as those discussed on claim 7 above, same rationale of rejection is applicable.

Regarding Claim 14, Donaldson discloses a method for a receiving networked computer system with an Internet connection

a mail transport agent MTA_1 (1402 of fig. 13), an Internet address IP_1 (e.g., destination IP address discussed in col.3, lines 5-7), recipient A_1 (e.g., the address to the local MTA, 1402 of fig.13, in step 1403, col.13, lines 26-29), and

an operating system (1090 of Fig. 7) capable of executing the method to reject (filter) unsolicited messages from

a transmitting networked computer system with an Internet connection (column 11, lines 13-33), and a message transfer agent MTA_0 (e.g., host 1400 of fig. 13) an Internet address IP_0 (e.g., the Proxy gets the IP address of the

host computer as shown in step 1404, of fig.14, col. 18, lines 5-7), sender_address A_0 (e.g., the proxy server processes the MAIL messages from the host, which contains the address of the purported sender of the incoming message, col.15, lines 62-64, and step 1404, fig.14), declared domain D_0 (e.g., domain name that was provided in the address of the purported sender of the incoming message from the remote host 1400, col.15, lines 3-4 and to the right of the "@"col.20, lines 4-5), and real domain DD_0 (e.g., verifies consistency of DNS information (i.e., declared domain) remote host, col.18, lines 11-14, and col.3, lines 5-6) comprising the steps of:

a) waiting for a new SMTP connection request (e.g. TCP connection to proxy (col. 15, lines 21-31);

b) relaying and monitoring the replies from MTA_0 to MTA_1 (e.g., proxy 1401, steps 1455-1459, and 1466 in fig. 18, shows the relaying of the replies from MTA_0 to MTA_1, where the proxy acting as a conventional firewall configuration i.e., monitors transfers of information, between MTA_0 (e.g., a remote host) and a MTA_1 (e.g., local MTA) (col.8, lines 25-28);

c) relaying replies from MTA_1 to MTA_0 (see fig.13 and note below) (e.g., the proxy awaits for the response MTA_1's response (e.g., local MTA) from the MAIL FROM message and writes the response immediately to the MTA_0 (e.g., remote host) in steps 1475 in fig. 20, col. 34, lines 3-5);

c') allowing MTA_1 to control the interaction between MTA_0 and MTA_1 until a RCPT reply is received from MTA_0 (col. 3, lines 51-60, col.8, lines 21-24,

col.9, lines 19-27, col.14, lines 5-22, col.17, lines 45-54, and col.36, lines 6-15, and *see* fig.25);

d) intercepting (receives) the RCPT reply from MTA_0 to MTA_1 (e.g., the proxy receives the RCPT command of a message from host 1400, by determining if the message's MAIL FROM address is trusted as discussed above, also col. 3, lines 51-60, col.8, lines 21-24, col.9, lines 19-27, col.14, lines 5-22, col.17, lines 45-54, and col.36, lines 6-15, and *see* fig.25);

e) determining if the message is unsolicited by analyzing the monitored replies (the proxy determines if the communication contains an unsolicited message by determining if the email contains trusted addresses, where if it does not contain trusted addresses (e.g. trusted hosts or white-listed addresses) it is deemed junk mail, i.e., it contains addresses of the purported sender which is commonly forged in junk mail. col.15, lines 50-65);

f) releasing (transferring) the intercepted RCPT reply if the message is determined not to be unsolicited (steps 1631 and 1637, of fig. 26, col. 40, lines 29-34);and

g) sending a an error reply (e.g., response 550) to MTA_0 if the message is determined to be unsolicited (step 1655 of fig. 27);

h) rejecting the connection with MTA_0 is rejected before the data portion of the unsolicited message is transmitted if the message is determined unsolicited (e.g., proxy closes the connection when it suspects that a sender's address was forged, col.16, lines 56 or if the remote host address is blacklisted

the proxy closes the connection and exits without any email being transferred, col.19, lines 23-26).

Regarding Claim16, Donaldson discloses the method of claim 14 as discussed above. Donaldson further discloses wherein the determining comprises checking if the IP 0 is in a allow address database.

Regarding Claim 17, Donaldson discloses the method of claim 14 as discussed above. Donaldson further discloses wherein the determining comprises checking if IP_0 is in a prevent_address database (blacklist database 1095) (e.g., blacklist, identifies IP addresses of remote hosts that will be blocked immediately after they connect to the proxy server, col. 11, lines 62-63).

.

Regarding Claim 18, Donaldson discloses the method of claim 14 as discussed above. Donaldson wherein the determining comprises checking if IP_0 has a domain name entry DD_0 in a DNS database (configuration database 1098) (col.12, lines 1-4).

Regarding Claim 19, Donaldson discloses the method of claim 14 as discussed above. Donaldson further discloses wherein the determining comprises checking if the real domain DD 0 matches the domain of sender address A 0 and the domain of sender_address A_0 is in a suspect_domain

database (trusted database) (col.9, lines 19-27, and col.20, lines 44-67, and col.21, lines 1-31).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Donaldson in view of Andrews et al. (US 2003/0204569) (referred herein after as Andrews)

Regarding Claim 6, Donaldson does not explicitly disclose where an unsolicited rejecting communications processor further includes a bad_from database and wherein the determining means determines if a message is unsolicited by checking if the from-address A_0 is in the bad_from database.

However, Andrews in a similar field of endeavor, such as filtering e-mails, discloses where an unsolicited rejecting communications processor further includes a bad_from database (e.g., special folder with previous detected SPAM data, and SPAM classifiers, [0049]) and

wherein the determining means determines if a message is unsolicited by checking if the from-address A_0 is in the bad_from database (e.g., block 53 of fig.4, analyzes databases of SPAM and undesirable e-mail data as identified in

[0042] and checks to see if email has come from a suspicious sender as discussed in [0039]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made, to utilize the teachings of Andrews for determining if a message is unsolicited by checking a database in Donaldson system to be able to filter out the content of addresses and messages that are commonly used by spammers. One of the ordinary skill of the art at the time the invention was made would have been motivated to combine the teachings of Donaldson and Andrews to have a more effective filtering system to prevent communication with unsolicited messages.

10. Claims 8, 10, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Donaldson in view of Wilson (US 2004/0015554) (referred herein after as Wilson).

Regarding Claim 8, Donaldson, does not explicitly disclose wherein determining means determines if a message is unsolicited by checking if the from-address A_0 matches the to-address A_1.

However, Wilson in a similar field of endeavor, such as active e-mail filtering, discloses wherein determining means determines if a message is unsolicited by checking if the from-address A_0 matches the to-address A_1 (e.g., “From” address, is identical to the “To” address, then the message can be assumed to be junk, [0084], *see* fig.4 and 6 domains are to the right of the “@”, for examples of “To” and “From” addresses).

It would have been obvious to one of ordinary skill in the art at the time the invention was made, to utilize the teachings of Wilson in Donaldson to provide a proactive approach of filtering e-mails that contain the same address as the recipient. One of the ordinary skill of the art at the time the invention was made would have been motivated to combine the teachings of Donaldson and Wilson, to prevent spammers who have always used fake addresses to send SPAM and tried to confuse the users of the system by disguising the from addresses of the unsolicited messages, as being the same addresses for the users themselves.

Regarding Claim 10, the combined teachings of Donaldson and Wilson further disclose wherein the determining means determines if a message is unsolicited by checking if the declared domain D_0 of MTA_0 is the same as the domain D_1 of MTA_1 (e.g., “From” address, is identical to the “To” address, then the message can be assumed to be junk, [0084], *see* fig.4 and 6 for examples of “To” and “From” addresses).

Regarding Claim 20, the combined teachings of Donaldson and Wilson further disclose wherein the determining comprises checking if the declared domain D 0 of MTA 0 does not match the real domain DD 0 (e.g., “From” address, is identical to the “To” address, then the message can be assumed to be junk, [0084], *see* fig.4 and 6 for examples of “To” and “From” addresses).

and the declared domain D_0 is in the suspect_domain database (trusted database) (col.9, lines 19-27, and col.20, lines 44-67, and col.21, lines 1-31).

11. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Donaldson in view of Levosky (US 2002/0087641) (referred herein after as Levosky).

Regarding Claim 12, Donaldson teaches a rejected_connection database (e.g. System Log, element 1099, of fig.7, col.12, lines 19-20), which logs the from-address A_0, to-address A_1, (e.g., at step 1408, of element 1401 in fig.14, logs entries of rejected_connections which inherently includes the data (e.g., from-address A_0, to-address A_1) gained from the previous filtering steps) and the reason for the rejection (e.g., sets a status zero, if the connection is good and sets an error number to indicate the specific error for a connection, col. 21, lines 14-17) if a message is rejected if the message is determined to be unsolicited. Donaldson does not explicitly disclose wherein the rejected_connection database logs time.

However, Levosky, in a similar field of endeavor, such as a system and method for controlling and organizing email to prevent SPAM abuse, discloses a rejected_connection data base (e.g., log) which logs all relevant information pertaining to the message (e.g., e-mail) transaction including time, date, addresses and identification information of the message (abstract, and [0017 and 0063]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made, to utilize the teachings of Levosky in Donaldson to have a

database that contains an accurate and exact log of the rejected connections, with the reasons, and time of each of the rejections. One of the ordinary skill of the art at the time the invention was made would have been motivated to combine the teachings of Donaldson and Levosky to allow the users of the system to be able to take a proactive approach in preparing for future SPAM attacks, by analyzing the reasons and the time periods that these transactions are taken place.

Regarding Claim 13, the combined teachings of Donaldson and Levosky further teach an allowed_connection database (Donaldson: e.g. System Log, element 1099, of fig.7, col.12, lines 19-20, also logs entries of allowed_connections, so that they can be added to the no_filter database (e.g., whitelist) as discussed in col. 20, lines 59-63), which logs the time (Levosky: e.g., all relevant information pertaining to the message transaction including time, date, addresses and identification information of the message is logged, (abstract, and [0017 and 0063]) and to-address A_1 (Donaldson: e.g., the address to the local MTA, fig.13, element 1402, in step 1403, col.13, lines 26-29, is logged and gets a status zero, for having a good connection, col.21, lines.14-17) if the message is determine not to be unsolicited.

12. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Donaldson, Andrews, Levosky in view of Wilson and in further view of Postel in RFC 821, Simple Transfer Protocol, referred here after as Postel.

Regarding Claim 15, the combined teachings of Donaldson and Andrews as described above, discloses a method for

a receiving networked computer system with an Internet connection, a mail transport agent MTA_1 (Donaldson: e.g., local MTA, fig.13, element 1402), IP address IP_1 (Donaldson: e.g., destination IP address as taught in col.3, lines 5-6), a domain name D_1, a to-address A_1 (Donaldson: e.g., the address to the local MTA, fig.13, element 1402, in step 1403, col.13, lines 26-29),

an allow_address database (Donaldson: e.g., trusted database, is used to identify trusted networks (IPs) that are permitted to bypass further filtering, col.11, lines 58-60, fig.7, element 1093);

a prevent address database (Donaldson: e.g., black list, identifies IP addresses of remote hosts that will be blocked immediately after they connect to the proxy server, col.11, lines 21-23, fig.7, element 1095),

a suspect_domain database (Donaldson: e.g., configuration database, col.16, lines 20-31),

a bad_from database (Andrews: e.g., block 53 of fig.4, analyzes databases of SPAM as discussed in [0042] and checks to see if email has come from a suspicious sender [0039]),

a no_filter database (Donaldson: e.g., whitelist database contains individual email addresses that are permitted to bypass further filtering, col.11 and lines 60-62, element 1094, fig.7) ,

a rejected_connection database, an allowed_connection database (Donaldson: e.g., System Log, element 1099, of fig.7, includes rejected/connected connections entries that are logged in the System Log, col.12, lines 19-20), and

an operating system (1090 of Fig. 7) capable of executing the method to reject unsolicited messages from a transmitting networked computer system with an Internet connection (Donaldson: e.g., Operating System, element 1090, of fig.7),

a message transfer agent MTA_0 (Donaldson: e.g., remote host, fig.13, element 1400), an IP address of IP_0 (Donaldson: e.g., proxy gets the IP address of the remote host computer as shown in step 1404, of fig.14, col. 18, lines 5-7),

a declared domain name D_0 (e.g., domain name that was provided in the address of the purported sender of the incoming message from the remote host 1400, col.15, lines 3-4 and to the right of the "@"col.20, lines 4-5), and real domain of DD_0 (e.g., verifies consistency of DNS information (i.e., declared domain) remote host, col.18, lines 11-14), , and a sender address of A_0 (e.g., the proxy server processes the MAIL messages from the remote host 1400, which contains the address of the purported sender of the incoming message, col.15, lines 62-64, and step 1404, fig. 14);

As related to steps: a, b, c, h, i, j, u, aa, ii, mm, nn, ss, aaa, ddd, oo, and qq, Donaldson and Andrews discloses a different order of communications which include the steps of:

- waiting for a SMTP connection request on the receiving networked computer system's Internet connection (Donaldson: see fig.2, step 1010);

- sending a 220 reply to MTA_0 to acknowledge the requested connection (Donaldson: see fig.2, step 1011);

- extracting IP address IP_0 from the connection request (Donaldson: see fig.14, step 1404);

- requesting a connection with MTA_1 (Donaldson: see fig.2, step 1010);

- waiting for a 220 reply from MTA_1 to acknowledge the requested connection (Donaldson: see fig.2, step 1011);

- waiting for a reply from either MTA_0 or MTA_1 (Donaldson: see fig.13 and note below);

- extracting domain D_0 from the reply (Donaldson: col.28, lines 38-45);

- extracting from-address A_0 (Donaldson: see fig.15, step 1414);

- extracting to-address A_1 (Donaldson: see fig.13, step 1480);

- rejecting the connection to MTA_0 by sending a 550 reply to MTA_0 (see fig.14, step 1408);

- waiting for a 354 reply from MTA_1 (Donaldson: see fig.2, step 1019 and note below);

- relaying the 354 reply from MTA_1 to MTA_0 (Donaldson: see fig.2, step 1019 and note below);

- waiting for a 250 reply from MTA_1 (Donaldson: see fig.18, fig.2, step 1022 and note below);

- waiting for 221 reply from MTA_1 (Donaldson: see fig.2 and note below);

- sending a 500 reply to MTA_0 to signal a syntax error (Donaldson: see note below);

- waiting for the data from MTA_0 (Donaldson: see fig.2, step 1018, fig.13, step 1484, and note below);

-waiting for a .\r\n from MTA_0 (Donaldson: see fig.2, step 1021,fig.13, step 1495, and note below).

Donaldson further discloses that regarding the active filtering overview, that although some of the status responses or error conditions are not illustrated, they're nonetheless understood to be part of the standard status responses and errors conditions of SMTP protocol (leyend of Fig. 13). Fig. 2 also provides additional help in the clarity of the purposes of these standard status responses and error conditions of the standard SMTP protocol.

Regarding steps: d, e, f, g, o, q, v, and bb, the combined teachings of Donaldson (col.16, lines 20-31) and Andrews further discloses a different order of communications, which include the steps of:

- testing if the DNS database has a domain name DD_0 for IP_0 (Donaldson: see Claim 5 above);

- testing if IP_0 is in an open relay database (Donaldson: see Claim 4 above);

- testing if IP_0 is in the allow_address database (Donaldson: see Claim 2 above);

- testing if IP_0 is in the prevent_address database (Donaldson: see Claim 3 above),

- testing if declared domain D_0 does not match real domain DD_0 of MTA_0

AND declared domain D_0 is in the suspect_domain database (Donaldson: *see* Claim 7 above);

- testing if A_0 is in the bad_from database (Donaldson: see Claim 6 above);

- testing if A_1 is in no_filter database (Donaldson: see Claim 9 above).

Also, regarding steps ee) and hh), the combined teachings of Donaldson/Andrews discloses logging the to-address A_1 (Donaldson: e.g., the address to the local MTA, fig.13, element 1402, in step 1403, col.13, lines 26-29, is logged and gets a status zero, for having a good connection, col.21, lines.14-17) in the allowed_connection database (Donaldson: e.g., System Log, element 1099, of fig.7, col.12, lines 19-20, also logs entries of allowed_connections, so that they can be added to the no_filter database (Donaldson: e.g., whitelist) as discussed in col. 20, lines 59-63) and logging the from-address A_0, to-address A_1 (Donaldson: e.g., at step 1408, of element 1401 in fig.14, logs entries of rejected_connections which inherently includes the data (Donaldson: e.g., from-address A_0, to-address A_1) gained from the previous filtering steps), and the reason for rejecting the connection (Donaldson: e.g., sets a status zero, if the connection is good and sets an error number to indicate the specific error for a

connection, col. 21, lines 14-17) in the rejected_connection database system. The Donaldson/Andrews system does not explicitly disclose the logging of time.

However, Levosky discloses an unsolicited rejecting communications processor that logs time in a connection_database (abstract, and [0017 and 0063]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made, to utilize the teachings of Levosky in the Donaldson/Andrews system to have a database that contains an accurate and exact log of the rejected connections, with the reasons, and time of each of the rejections to provide accurate and efficient analysis of SPAM attacks on the system at a specific time. One of the ordinary skill of the art at the time the invention was made, would have been motivated to combine the teachings of Donaldson/Andrews and Levosky in the interest of allowing the users of the system to be able to take a proactive approach in preparing for future SPAM attacks, by analyzing the reasons and the time periods that these transactions are taken place. Thus, the combined teachings of the Donaldson/Andrews and Levosky system suggest the methods substantially as claimed.

Also, regarding steps: p) and cc), the combined teachings of the Donaldson/Andrews/Levosky system does not explicitly disclose testing if declared domain D_0 of MTA_0 matches domain D_1 of MTA_1 and testing if A_0 matches A_1.

However, Wilson discloses an unsolicited rejecting communications processor that tests if the declared domain D_0 of MTA_0 matches domain D_1

of MTA_1 and if A_0 matches A_1 (e.g., “From” address, is identical to the “To” address, then the message can be assumed to be junk, par [0084], in which the address also includes the domain (e.g., to the right of the “@”) as discussed in par [0082]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made. One to utilize the teachings of Wilson in the Donaldson system to provide a way of filtering messages that contains the same destination information as the receiving user. One of the ordinary skill of the art at the time the invention was made would have been motivated to combine the teachings of the Donaldson, Andrews, and Levosky with Wilson’s teachings to be able to test messages that contain the same information as the receivers of these messages to help protect against this unique technique being used by spammers in order to protect the users of the system from accidentally effecting their own systems, by thinking that they may have safely messaged themselves.

In further the combined teachings of Donaldson/Andrews/Levosky/Wilson teach the step w):

- testing if DD_0 does not match the domain of A_0 (Wilson: e.g., “From” address, is identical to the “To” address, then the message can be assumed to be junk, [0084], *see* fig.4 and 6 for examples of “To” and “From” addresses) and the domain of A_0 is in the suspect_domain database (Donaldson: *see* Claim 7 above);

Regarding further limitation(s):

The above-mentioned prior art does not explicitly check for SMTP commands RSET, SEND, SOML, SAML, VRFY, NOOP, EXPN, HELP, or TURN, as recited in step vv.

However, Postel, in a similar field of endeavor, such as the use of Simple Mail Transfer Protocol, teaches that the objective of SMTP is to transfer mail reliably and efficiently, and that it only requires a reliable ordered data stream channel.

Postel discloses where SMTP is capability of relaying e-mail message across different transport service environments. A transport service provides an inter-process communication environment and it may cover one network, several networks, or a subset of a network. A process can communicate directly with another process through any mutually known inter-process communication environment, and a host on different transport systems can relay mail (see page 5).

Postel further teaches the commands as recited in step vv), RSET, SEND, SOML, SAML, VRFY, NOOP, EXPN, HELP, or TURN (see pages 8,11, 25-27).

Postel also discloses that in order to make SMTP workable, the minimum implementation for all receivers (e.g., MTA_0 and MTA_1) is that they must be compatible with at least the SMTP protocol commands: HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT (see page 41).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made, to use the features and commands of the SMTP protocol in an attempt to jump and relay the communication to provide an

effective filtering method to prevent the communication of SPAM between two message transfer agents, as a person with ordinary skill has a good reason to pursue the known features and implementations of the SMTP protocol and it's commands, within his or her technical grasp. In turn, because it would have been obvious to perform the steps in the order recited by the applicant to prevent the further communication of SPAM. One of the ordinary skill of the art at the time the invention was made would have been motivated to combine the teachings of the Donaldson system with Postel to be able to implement and perform the steps of jumping and relaying of the SMTP protocols to satisfy the needs of a particular inter-process communication environment and to optimize the system resources for the filtering of SPAM in this particular environment.

In further regarding the further limitations, the combined teachings of Donaldson, Andrews, Levosky, Wilson, and Postel teach the steps wherein:

-t_allow represents the results of the testing in step (f) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

- t_no filter represents the results of the testing in step (bb) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

- t_prevent represents the results of the testing in step (g) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

- t_open represents the results of the testing in step (e) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

- t_DD represents the results of the testing in step (d) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

- t_bad_from represents the results of the testing in step (v) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

- t_suspect_domain represents the results of the testing in step (w) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

- t_echo_domain represents the results of the testing in step (p) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

-t to from represents the results of the testing in step (cc) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45); and

-t_forged_domain represents the results of the testing in step (q) (Donaldson: col.40, lines 3-5, lines 6-7, and 41-45);

Response to Amendments

13. Amendment to the abstract in response to examiner's objection has been considered. The amendment obviates previously raised objection, as such this objection hereby withdrawn.

Amendment to the specification in response to examiner's objection has been considered. The amendment obviates previously raised objection, as such this specification hereby withdrawn.

Amendment to the drawings in response to examiner's objection has been considered. The amendment obviates previously raised objection, as such this objection hereby withdrawn.

Response to Arguments

14. Applicant's arguments filed 14 January 2008 have been fully considered but they are not persuasive.

A) As to claim 1, Applicant argues that Claim 1, Donaldson does not disclose, teach, or suggest an unsolicited message rejecting communications processor including the step "whereby the interaction between MTA_0 and MTA_1 before a RCPT command from MTA_0 is received by the unsolicited message rejecting communications processor." Applicant further argues that the Active Filter proxy and not MTA_1 controls the interaction between MTA_0 and MTA_1 before a RCPT command from MTA_0 is received by the unsolicited message rejecting processor.

As to the above point A), the Examiner respectfully disagrees in that Donaldson *does* disclose, teach, or suggest an unsolicited message rejecting communications processor (proxy 1401) that further includes the step "whereby the interaction between MTA_0 and MTA_1 before a RCPT command from MTA_0 is received by the unsolicited message rejecting communications processor" and further discloses that MTA_1 controls the interaction between MTA_0 and MTA_1 before a RCPT command from MTA_0 is received by the unsolicited message rejecting processor (col. 3, lines 51-60, col.8, lines 21-24, col.9, lines 19-27, col.14, lines 5-22, col.17, lines 45-54, and col.36, lines 6-15). Donaldson suggests that the unsolicited message rejecting communications processor may operate at the MTA level and is compatible with all known SMTP MTAs therefore, it would be able to perform the same functionalities of the disclosed MTAs. In further, Donaldson suggests that the MTA may also provide control by implementing other conventional spam-filtering methods of its own (col.8, lines 21-24, and col.9, lines 23-26). One of ordinary skill in the art at the time the invention was made, would have appreciated that a Proxy may operate anywhere within the network as well.

B) As to Claim 7, Applicant argues that Donaldson fails to disclose, teach or suggest each limitation of Claim 7. In further, Applicant alleges that claim 7 as amended is not anticipated by Donaldson because Donaldson fails to disclose the additional limitation steps "further includes a suspect_domain database and wherein the determining means determines if a message is unsolicited by

checking if the real domain DD_0 matches the domain of sender A_0 and the domain of sender_address A_0 is in the suspect_domain database".

As to point B), the Examiner respectfully disagrees in that Donaldson *does* disclose, teach or suggest each limitation of Claim 7, which include the additional limitation steps, "further includes a suspect_domain database and wherein the determining means determines if a message is unsolicited by checking if the real domain DD_0 matches the domain of sender A_0 and the domain of sender_address A_0 is in the suspect_domain database" (col.16, lines 20-31, col.15, lines 60-67, and col.16, lines 1-4). The proxy can be configured to perform different types of testing. Therefore, the configuration database can be configured to contain suspected sender_addresses which will trigger a flag to true, if the sender address A_0 matches one listed in the configuration database. The proxy in further performs open reverse test connections to determine if the address of the purported sender is legitimate. Applicant's arguments that a reverse test connection that is used by Donaldson to verify that a connection exists is a *far cry* from checking that a real domain matched the domain of a sender address, fail to comply with 37 C.F.R. 1.111 (b) because they amount to a general allegation in that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Applicant is advised to be more specific when arguing a specific distinction between the cited reference and the claimed invention.

C) As to Claim 9, Applicant argues that Donaldson fails to disclose, teach, or suggest each limitation of Claim 9. In further, Applicant alleges that claim 9 as amended is not anticipated by Donaldson because Donaldson fails to disclose the additional limitation step “checking if the recipient A_1 is in the no_filter database” and further fails to even disclose a "no_filter database”.

As to point C), the Examiner respectfully disagrees in that Donaldson *does* disclose, teach, or suggest each limitation of Claim 9, which include the additional limitation step “checking if the recipient A_1 is in the no_filter database” and further fails to even disclose a "no_filter database” (col.37, lines 29-32). The recipient whitelist database is flexible that allows users to define their own filtering policies. Therefore, a user can use this whitelist database to implement how filtering will be performed, as desired.

D) As to Claim 11, Applicant argues that Donaldson fails to disclose, teach, or suggest each limitation of Claim 11. In further, Applicant alleges that claim 11 as amended is not anticipated by Donaldson because Donaldson fails to disclose the additional limitation "checking if the declared domain D_0 is in the suspect_domain database." In particular, the applicant argues that although Donaldson processes the command, Donaldson fails to derive the any information from the command.

As to point D), the Examiner respectfully disagrees in that Donaldson *does* disclose, teach, or suggest each limitation of Claim 11 which include the additional limitation checking if the declared domain D_0 is in the

suspect_domain database" (col.16, lines 20-31, col.15, lines 60-67, and col.16, lines 1-4). The proxy can be configured to perform different types of testing. Therefore, the configuration database can be configured to contain suspected domains which will trigger a flag to true, if the declared domain D_0 matches one listed in the configuration database. In further, Donaldson *does* disclose that the proxy derives (reads) information through the HELO command (col.28, lines 33-34).

E) As to Claim 14, Applicant argues that claim 14 is not anticipated by Donaldson because Donaldson fails to disclose "allowing MTA_1 to control the interaction between MTA_0 and MTA_1 until a RCPT reply is received from MTA_0." In further, applicant alleges that claim 14 as amended is not anticipated by Donaldson, because the previous limitation version of step (c') in the form of a whereby clause is incorrect, and specifically that in Donaldson, prior to the RCPT command the active filter proxy is handling the SMTP messages on behalf of the local MTA, therefore the active filter proxy is not allowing the local MTA to control the interaction between the sending MTA and local MTA.

As to point E), the Examiner respectfully disagrees in that Donaldson *does* disclose the limitation step "allowing MTA_1 to control the interaction between MTA_0 and MTA_1 until a RCPT reply is received from MTA_0." (col. 3, lines 51-60, col.8, lines 21-24, col.9, lines 19-27, col.14, lines 5-22, col.17, lines 45-54, and col.36, lines 6-15). Donaldson suggests that the unsolicited message rejecting communications processor may operate at the MTA level and is

compatible with all known SMTP MTAs therefore, it would be able to perform the same functionalities of the disclosed MTAs. In further, Donaldson suggests that the MTA may also provide control by implementing other conventional spam-filtering methods of its own (col.8, lines 21-24, and col.9, lines 23-26). One of ordinary skill in the art at the time the invention was made, would have appreciated that a Proxy may operate anywhere within the network as well. In further, the previous limitation version of step (c') in the form of a whereby clause is indeed disclosed by Donaldson (col. 3, lines 51-60, col.8, lines 21-24, col.9, lines 19-27, col.14, lines 5-22, col.17, lines 45-54, and col.36, lines 6-15).

F) As to Claims 8 and 10, Applicant argues that Donaldson in further view of Wilson fails to disclose the step that "determines if a message is unsolicited by checking if the declared domain D_0 of MTA_0 is the same as the domain D_1 of MTA_1". Applicant further argues that the cited refers to the "FROM" and "TO" addresses and not to the domains declared or announced by an MTA.

As to point F), the Examiner respectfully disagrees in that the combined teachings of Donaldson in view of Wilson *do* disclose the step that "determines if a message is unsolicited by checking if the declared domain D_0 of MTA_0 is the same as the domain D_1 of MTA_1" (Wilson: e.g., "From" address, is identical to the "To" address, then the message can be assumed to be junk, [0084], *see* fig.4 and 6 for examples of "To" and "From" addresses). The combined teachings of Donaldson and Wilson further teach that the "FROM" and "TO" contain the

domains declared or announced by an MTA (Wilson: e.g., domains are to the right of the “@”, *see* fig.4 and 6 for examples of "TO" and "FROM" addresses).

G) As to Claim 15, Applicant argues that the combination of Donaldson, Andrews, Levosky, Wilson, and Postel *does* not disclose, in particular Donaldson, does not teach or suggest the features and limitations of steps o, p, q, r, w, x, bb, dd, and vv. Specifically, for step o), the combination of Donaldson, Andrews, Levosky, Wilson, and Postel , in particular Donaldson, fails to disclose getting a domain name. Applicant further argues that the hostname in the combination of Donaldson, Andrews, Levosky, Wilson, and Postel is equated with the domain name, and the domain name would not be extracted from the reply and the “domain name” that is disclosed in the combination of Donaldson, Andrews, Levosky, Wilson, and Postel is the real_domain DD_0 and not the declared domain D_0.

In further, Applicant argues that in steps r and x, the combination of Donaldson, Andrews, Levosky, Wilson, and Postel, in particular Donaldson does not relay any of the commands from MTA_0 to MTA_1 until after the RCPT command where it may operate in pass-through.

As to point G), In response to the applicant’s arguments against the reference of Donaldson individually, of the highlighted features and limitations disclosed in the steps of: o, p, q, bb, dd, and vv, one cannot show

nonobviousness by attacking references individually where the rejections are based on combination of references.

Examiner disagrees in that the combination of Donaldson, Andrews, Levosky, Wilson, and Postel *does* disclose In regards to the limitations of step o), the combined teachings of Donaldson, Andrews, Levosky, Wilson, and Postel, disclose getting a domain name (Donaldson: (e.g., configuration database, which includes general data such as permissible domain names, col.12, lines 1-4, col.16, lines 21-31) and in further, Donaldson *does* disclose that the proxy derives (reads) information through the HELO command (col.28, lines 33-34).

Also, in regards to the limitations of step w), testing if DD_0 does not match the domain of A_0 (Wilson: e.g., "From" address, is identical to the "To" address, then the message can be assumed to be junk, [0084], *see* fig.4 and 6 for examples of "To" and "From" addresses) is in the domain of A_0 is in the suspect_domain database (Donaldson: col.16, lines 20-31, col.15, lines 60-67, and col.16, lines 1-4);

In further, regarding steps r) and x), the combined teachings of Donaldson, Andrews, Levosky, Wilson, and Postel, *does* disclose relaying any of the commands from MTA_0 to MTA_1 until after the RCPT command where it may operate in pass-through (Donaldson: (col. 3, lines 51-60, col.8, lines 21-24, col.9, lines 19-27, col.14, lines 5-22, col.17, lines 45-54, and col.36, lines 6-15).

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

16. Reply to a final rejection or action must include cancellation of, or appeal from the rejection of, each rejected claim. If any claim stands allowed, the reply to a final rejection or action must comply with any requirements or objections as to form (see 1.113). If prosecution in an application is closed, an applicant may request continued examination of the application by filing a submission and the fee set forth in § 1.17(e) prior to the earliest of: (c) A submission as used in this

section includes, but is not limited to, an information disclosure statement, an amendment to the written description, claims, or drawings, *new arguments, or new evidence in support of patentability*. If reply to an Office action under 35 USC 132 is outstanding, the submission must meet the reply requirements of § 1.111 (see MPEP 706.07)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY MEJIA whose telephone number is (571)270-3630. The examiner can normally be reached on Mon-Thur 9:30AM-8:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

Anthony Mejia
Patent Examiner

/Salad Abdullahi/

Primary Examiner, Art Unit 2157